View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by University of Michigan School of Law

University of Michigan Journal of Law Reform

Volume 50

2017

Human Rights and Cybersecurity Due Diligence: A Comparative Study

Scott J. Shackelford
Indiana University Kelley School of Business

Follow this and additional works at: https://repository.law.umich.edu/mjlr

 Part of the Business Organizations Law Commons, Human Rights Law Commons, and the Internet Law Commons

Recommended Citation

Scott J. Shackelford, *Human Rights and Cybersecurity Due Diligence: A Comparative Study*, 50 U. MICH. J. L. REFORM 859 (2017).
Available at: https://repository.law.umich.edu/mjlr/vol50/iss4/1

This Article is brought to you for free and open access by the University of Michigan Journal of Law Reform at University of Michigan Law School Scholarship Repository. It has been accepted for inclusion in University of Michigan Journal of Law Reform by an authorized editor of University of Michigan Law School Scholarship Repository. For more information, please contact mlaw.repository@umich.edu.

HUMAN RIGHTS AND CYBERSECURITY DUE DILIGENCE: A COMPARATIVE STUDY

Scott J. Shackelford JD, PhD*

ABSTRACT

No company, just like no nation, is an island in cyberspace; the actions of actors from hacktivists to nation-states have the potential to impact the bottom line, along with the human rights of consumers and the public writ large. To help meet the multifaceted challenges replete in a rapidly globalizing world—and owing to the relative lack of binding international law to regulate both cybersecurity and the impact of business on human rights—companies are reconceptualizing what constitutes "due diligence." This Article takes lessons from both the cybersecurity and human rights due diligence contexts to determine areas for cross-pollination in an effort to provide firms with a more comprehensive view of due diligence best practices divorced from a particular technological or cultural context. In so doing, this Article uses the Guiding Principles on Business and Human Rights as a starting point, marrying this framework with the relevant cybersecurity literature and the overarching analytical framework of polycentric governance. Ultimately, this Article argues that organizations should take a wider view of enterprise risk management that combines their cybersecurity and human rights aspirations given the growing extent to which these fields are becoming interlinked under the umbrella of sustainable development.

INTRODUCTION 860
I. DEFINING KEY TERMS 862
A. *The Multifaceted Cyber Threat Facing the Private Sector and "Cyber Peace"* 862
B. *Global Approaches to "Sustainable Development"* 865
C. *Introducing Polycentrism* 867
II. HUMAN RIGHTS DUE DILIGENCE PRIMER 868
III. UNPACKING CYBERSECURITY DUE DILIGENCE 874
IV. LINKING HUMAN RIGHTS AND CYBERSECURITY UNDER SUSTAINABLE DEVELOPMENT 879
CONCLUSION 883

* Associate Professor of Business Law and Ethics, Indiana University Kelley School of Business; Senior Fellow, Center for Applied Cybersecurity Research; Research Fellow, Harvard Belfer Center on Science and International Affairs; Director, Ostrom Workshop Program on Cybersecurity and Internet Governance.

> *"Companies have a responsibility to respect human rights, which means to act with due diligence to avoid infringing on the rights of others."*[1]

INTRODUCTION

No company, just like no nation, is an island in cyberspace; the actions of actors from hacktivists to nation states have the potential to impact the bottom line, along with the human rights of consumers and the public writ large. A case in point is the alleged Russian penetration of the Democratic National Committee's servers during the 2016 campaign, raising the specter of cyber insecurity, civil rights violations, and rising geopolitical tensions in a single episode.[2] To help meet the multifaceted challenges replete in a rapidly globalizing world—and owing to the relative lack of binding international law regulating both cybersecurity and the intersection of business on human rights—companies and countries are reconceptualizing what constitutes "due diligence."[3] This Article takes lessons from both the cybersecurity and human rights due diligence contexts to determine areas for cross-pollination in an effort to provide firms with a more comprehensive view of due diligence best practices divorced from a particular technological or cultural context.[4] In so doing, this Article uses the Guiding Principles on Business and Human Rights[5] as a starting point, marrying this

---

1. INST. FOR HUMAN RIGHTS & BUS., THE "STATE OF PLAY" OF HUMAN RIGHTS DUE DILIGENCE: ANTICIPATING THE NEXT FIVE YEARS, 1 (2011), http://www.ihrb.org/pdf/The_State_of_Play_of_Human_Rights_Due_Diligence.pdf.

2. *See* Ellen Nakashima, *Russian Government Hackers Penetrated DNC, Stole Opposition Research on Trump*, WASH. POST (June 14, 2016), https://www.washingtonpost.com/world/national-security/russian-government-hackers-penetrated-dnc-stole-opposition-research-on-trump/2016/06/14/cf006cb4-316e-11e6-8ff7-7b6c1998b7a0_story.html.

3. *See* Jamie D. Prenkert & Scott J. Shackelford, *Business, Human Rights, and the Promise of Polycentricity*, 47 VAND. J. TRANSNAT'L L. 451, 452 (2014).

4. *See, e.g.*, *Human Rights Due Diligence*, BUS. & HUMAN RTS. RES. CTR., http://business-humanrights.org/en/un-guiding-principles/implementation-tools-examples/implementation-by-companies/type-of-step-taken/human-rights-due-diligence (last visited Apr. 16, 2017) ("According to the UN Guiding Principles Reporting Framework, human rights due diligence is: *'An ongoing risk management process . . . in order to identify, prevent, mitigate and account for how [a company] addresses its adverse human rights impacts. It includes four key steps: assessing actual and potential human rights impacts; integrating and acting on the findings; tracking responses; and communicating about how impacts are addressed.'"*). This approach was chosen given the tendency of organizations to consider due diligence from an, at times, myopic lens that can be far too narrow given the multifaceted risks facing firms. *See, e.g.*, Peter Howson, *Identifying and Minimizing the Strategic Risks from M&A, in* APPROACHES TO ENTERPRISE RISK MANAGEMENT 153, 154 (2010).

5. *See, e.g.*, JOHN G. RUGGIE, JUST BUSINESS: MULTINATIONAL CORPORATIONS AND HUMAN RIGHTS 78 (2013) ("The overriding lesson I drew . . . was that a new regulatory dynamic was

framework with the relevant cybersecurity literature[6] and the overarching analytical framework of polycentric governance. Ultimately, this Article argues that organizations should take a wider view of enterprise risk management that combines their cybersecurity and human rights aspirations given the growing extent to which these fields are becoming interlinked under the umbrella of sustainable development.[7]

This Article is structured as follows. Part I begins the analysis by defining key terms including cyber peace, sustainable development, and polycentric governance. Part II centers on the concept of human rights due diligence focusing on the Ruggie Framework. Part III builds from the discussion of human rights and discusses the emerging field of cybersecurity due diligence, with special attention being paid to how the concept is being operationalized in the public and private sectors. Finally, Part IV concludes the comparative analysis and discusses the extent to which human rights and cybersecurity are cross pollinating, emphasizing what that

---

required under which public and private governance systems . . . each come to add distinct value, compensate for one another's weaknesses, and play mutually reinforcing roles—out of which a more comprehensive and effective global regime might evolve, including specific legal measures. International relations scholars call this 'polycentric governance.'").

6. *See* Scott J. Shackelford, Scott Russell & Andreas Kuehn, *Unpacking the International Law on Cybersecurity Due Diligence: Lessons from the Public and Private Sectors*, 17 CHI. J. OF INT'L L. 1 (2016); Scott J. Shackelford & Scott Russell, *Operationalizing Cybersecurity Due Diligence: A Transatlantic Case Study*, 67 S.C. L. REV. 609 (2016).

7. *See, e.g.*, INT'L TELECOMM. UNION, *Action Line C5 (Building Confidence and Security in the Use of ICTs)—National Cybersecurity Strategies for Sustainable Development*, WSIS FORUM, https://www.itu.int/net4/wsis/forum/2016/Agenda/Session/120 (last visited Apr. 16, 2017). Although the topic of human rights due diligence has received attention in the literature, the intersection with cybersecurity and Internet governance has been underappreciated. *See, e.g.*, Larry Cata Backer, *From Institutional Misalignments to Socially Sustainable Governance: The Guiding Principles for the Implementation of the United Nations' "Protect, Respect and Remedy" and the Construction of Inter-Systemic Global Governance*, 25 PAC. MCGEORGE GLOBAL BUS. & DEV. L.J. 69, 85 (2012) ("This focus suggested both the governance character of the device - human rights due diligence was the expression of the "law" of corporate behavior within its operational framework - and the means through which it could enforce its norms and connect them to the governance systems of states and international actors."). *Cf.* Oren Gross, *Cyber Responsibility to Protect: Legal Obligations of States Directly Affected by Cyber-Incidents*, 48 CORNELL INT'L L.J. 481, 494 (2015) (discussing conceptions of cybersecurity due diligence but neglecting its intersection with human rights). "Sustainable development" is discussed in detail in Part I(B). *See Topic: Sustainable Development*, INT'L INST. FOR SUSTAINABLE DEV., http://www.iisd.org/topic/sustainable-development (last visited Apr. 16, 2017) ("Sustainable development is development that meets the needs of the present without compromising the ability of future generations to meet their own needs. It contains within it two key concepts: the concept of needs, in particular the essential needs of the world's poor, to which overriding priority should be given; and the idea of limitations imposed by the state of technology and social organization on the environment's ability to meet present and future needs.").

portends for the future of both due diligence and sustainable development and how firms should use this combined, more holistic, framework for business decision-making.

I. DEFINING KEY TERMS

In order to proceed with the analysis, it is important first to define key terms to provide framework for discussion. This Part proceeds by first introducing the multifaceted cyber threat and the concept of cyber peace before moving on to discuss the concepts of due diligence, sustainable development, and polycentrism. Parts II and III will then build from this discussion by investigating the intersections between human rights and cybersecurity due diligence.

A. The Multifaceted Cyber Threat Facing the Private Sector and "Cyber Peace"

From vulnerabilities in the SWIFT system undergirding international finance, to attacks on critical infrastructure operated primarily by private firms, to smart phones that can be turned into microphones,[8] organizations of all sizes are increasingly in the cross-hairs of cyber attackers that can range from hacktivists to nation-states. Data on the number and type of cyber attacks impacting the private sector in particular is notoriously difficult to pin down. Companies rarely compile, organize, and transmit data on cyber attacks due in part to liability concerns.[9] This concern was addressed somewhat by the Cybersecurity Act of 2015, which among other things, laid out liability protections for firms that voluntarily share their cyber threat data with the federal government.[10] However, this congressional fix was far from the "comprehensive" bill originally envisioned, which is why President Obama had continued with executive action that, among other things, expanded public-private

8. *See* Trevor Hughes, *Anti-Virus Pioneer John McAfee: Your Phone may be Snooping on You*, USA TODAY (May 14, 2016, 5:59 PM), http://www.usatoday.com/story/tech/2016/05/11/anti-virus-pioneer-john-mcafee-warns-mobile-phone-snooping/84266838/ (noting that, according to John McAfee, "the danger comes from the camera and microphones we carry everywhere in our pockets, attached to our smartphones. It's a 'trivial' matter, he says, for a hacker to remotely and secretly turn on a phone's sensors.").

9. *See* SCOTT J. SHACKELFORD, MANAGING CYBER ATTACKS IN INTERNATIONAL LAW, BUSINESS, AND RELATIONS: IN SEARCH OF CYBER PEACE 202 (2014) [hereinafter MANAGING CYBER ATTACKS].

10. *See* Cybersecurity Information Sharing Act of 2015, S. 754, 114th Cong. (2015) (focusing on incentivizing information sharing to improve national cybersecurity).

information sharing and established the National Institute for Standards and Technology (NIST) Cybersecurity Framework comprised partly of private-sector best practices that companies could adopt to better secure critical infrastructure.[11] Although the U.S. Securities and Exchange Commission (SEC) published disclosure requirements back in 2011, it interpreted existing regulations broadly, requiring disclosure of "material" attacks leading to financial losses,[12] and suggested that more robust reporting requirements are in the pipeline.[13] Moreover, there is evidence that even for those firms that should be reporting such breaches to the SEC, they have not been doing so either because they were not aware of the breach (which is reportedly still the case in the majority of incidents) or because of a lack of enforcement mechanisms.[14]

Given the complexities inherent in mitigating cyber risk, more firms are moving from a reactive, defensive posture, to a proactive approach to cybersecurity risk management that includes a range of technological, organizational, and budgetary best practices.[15] Increasingly, these concepts are being bundled together within the growing literature on due diligence. While most of the attention on this concept initially came from the private sector, led by industries such as insurance, governments are also increasingly developing the concept, including the U.S. and Germany as is discussed further in Part III. Before turning to a full discussion of this concept,

---

11. *See* NAT'L INST. OF STANDARDS AND TECH., IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY EXECUTIVE ORDER 13636: PRELIMINARY CYBERSECURITY FRAMEWORK § 1.0, at 1 (2013), http://www.nist.gov/itl/upload/preliminary-cybersecurity-framework.pdf.

12. DIV. OF CORP. FIN., *CF Disclosure Guidance: Topic No. 2 Cybersecurity*, U.S. SEC. & EXCH. COMM'N, (Oct. 13, 2011), https://www.sec.gov/divisions/corpfin/guidance/cfguidance-topic2.htm; Joel Bronstein, *The Balance Between Informing Investors and Protecting Companies: A Look at the Division of Corporation Finance's Recent Guidelines on Cybersecurity Disclosure Requirements*, 13 N.C. J.L. & TECH. ON. 257, 271 (2012) (citing TSC Indus., Inc. v. Northway, Inc., 426 U.S. 438, 449 (1976), which defined "material" as "a substantial likelihood that the disclosure of the omitted fact would have been viewed by the reasonable investor as having significantly altered the 'total mix' of information made available.").

13. *See, e.g.*, *SEC Staff Provides Guidance on Disclosure Obligations Relating to Cybersecurity Risks and Cyber Incidents*, WSGR ALERT (Oct. 18, 2011), https://www.wsgr.com/publications/PDFSearch/wsgralert-cybersecurity-risks.pdf [hereinafter WSGR ALERT]; Chris Strohm, *SEC Chairman Reviewing Company Cybersecurity Disclosures*, BLOOMBERG (May 13, 2013, 3:01 PM), http://www.bloomberg.com/news/2013-05-13/sec-chairman-reviewing-company-cybersecurity-disclosures.html (reporting that the SEC is exploring strengthening cyber attack disclosure requirements).

14. *See* Joseph Menn, *Exclusive: Hacked Companies Still Not Telling Investors*, REUTERS (Feb. 2, 2012, 5:46 PM), http://www.reuters.com/article/us-hacking-disclosures-idUSTRE8110YW20120202.

15. For more on this topic, see MANAGING CYBER ATTACKS, *supra* note 9, at 210–30; Amanda Craig et al., *Proactive Cybersecurity: A Comparative Industry and Regulatory Analysis*, 18 AM. BUS. L.J. 721, 722 (2015).

though, it is important to understand the concepts of cyber peace, sustainable development, and polycentric governance.

The International Telecommunication Union (ITU), a UN specialized agency focusing on information and communication technologies (ICT), pioneered some of the early work in the field of cyber peace studies along with the Vatican and the World Federation of Scientists by defining the term in part as "a universal order of cyberspace" built on a "wholesome state of tranquility, the absence of disorder or disturbance and violence . . . ."[16] Although certainly desirable, such an outcome, e.g., the end of cyber attacks, is politically and technically unlikely, at least in the near term.[17] That is why cyber peace is defined here not as the absence of conflict, a state of affairs that may be more accurately called negative cyber peace.[18] Rather, it is the construction of a network of multilevel regimes that promote global, just, and sustainable cybersecurity by clarifying the rules of the road for companies and countries alike in order to help reduce the threats of cyber conflict, crime, and espionage to levels comparable to other business and national security risks.[19] To achieve this goal, a new approach to cybersecurity is needed that seeks out best practices from the public and private sectors to enhance cybersecurity due diligence. Working together through polycentric partnerships (defined in Part I(C)), we can mitigate the risk of cyber conflict by laying the groundwork for a positive cyber peace that respects human rights, spreads Internet access along with best practices, and strengthens governance mechanisms by fostering multi-stakeholder collaboration.[20] Already some of the public- and private-sector efforts may be bearing fruit with, by some estimates, the severity of cyber attacks

16. Henning Wegener, *Cyber Peace*, *in* HAMADOUN I. TOURÉ, THE QUEST FOR CYBER PEACE 77, 78 (2011), http://www.itu.int/dms_pub/itu-s/opb/gen/S-GEN-WFS.01-1-2011-PDF-E.pdf. (arguing that "unprovoked offensive cyber action, indeed any cyber attack, is incompatible with the tenets of cyber peace.").

17. To its credit, though, the ITU report recognizes this fact, and that the concept of cyber peace should be broad and malleable given an ever-changing political climate and cyber threat landscape. *Id.* at 78 ("The definition [of cyber peace] cannot be watertight, but must be rather intuitive, and incremental in its list of ingredients.").

18. The notion of negative peace has been applied in diverse contexts, including civil rights. *See, e.g.*, Martin Luther King, Jr., *Nonviolence and Racial Justice*, 74 CHRISTIAN CENTURY 165, 165 (1957) (arguing "[t]rue peace is not merely the absence of some negative force – tension, confusion or war; it is the presence of some positive force – justice, good will and brotherhood.").

19. For a more in-depth discussion of this topic, see the original publication of this conceptualization in the Foreword to MANAGING CYBER ATTACKS, *supra* note 9.

20. *See* Johan Galtung, *Peace, Positive and Negative*, *in* THE ENCYCLOPEDIA OF PEACE PSYCHOLOGY 1, 1 (Daniel J. Christie ed., 2011) (comparing the concepts of negative and positive peace).

beginning to plateau and "an emerging norm against the use of severe state-based cyber-tactics" evolving.[21] Further progress may be made by applying lessons learned from the sustainable development and polycentric governance contexts.

B. Global Approaches to "Sustainable Development"

Sustainable development has been defined by the UN Brundtland Report as "development that meets the needs of the present without compromising the ability of future generations to meet their own needs."[22] The term has found expression in all manner of legal instruments and civil society position papers at the national and international levels,[23] ranging from the 1946 International Convention for the Regulation of Whaling to the 1983 International Tropical Timber Agreement.[24] The concept has even found some traction in space law and policy circles. For example, international law requires States, "to avoid activities that would be harmful to the environment of the earth or to celestial bodies. . . ."[25] This 'no harm' provision is a key part of fostering both due diligence—as will be discussed in Parts II and III—as well as sustainable development in space, but it is also left largely undefined, like so much of space law. Limited progress was made by the UN General Assembly in 2010, which added the objective of sustainable development alongside international cooperation to foster the peaceful use of space.[26]

---

21. Brandon Valeriano & Ryan C. Maness, *The Coming Cyberpeace: The Normative Argument Against Cyberwarfare*, FOREIGN AFF. (May 13, 2015), https://www.foreignaffairs.com/articles/2015-05-13/coming-cyberpeace.

22. WORLD COMM'N ON ENV'T & DEV., OUR COMMON FUTURE, U.N. Doc. A/42/427, at 37 (1987) (1987), http://www.un-documents.net/our-common-future.pdf; *see also* Gabcikovo-Nagymaros Project (Hung. v. Slovk.), 1997 I.C.J. 7, 78 (Sept. 25) (defining sustainable development as "[the] need to reconcile economic development with protection of the environment[.]").

23. *See, e.g.*, JOHN PEZZEY, SUSTAINABLE DEVELOPMENT CONCEPTS: AN ECONOMIC ANALYSIS 55-62 (1992), http://documents.worldbank.org/curated/en/237241468766168949/pdf/multi-page.pdf.

24. Peter H. Sand, *Lessons Learned in Global Environmental Governance*, 18 B.C. ENVTL. AFF. L. REV. 213, 222 (1991).

25. James Kraska, *Indistinct Legal Regimes*, *in* SECURING FREEDOM IN THE GLOBAL COMMONS 49, 60 (Scott Jasper ed., 2010).

26. *See* G.A. Res. 64/86, International Cooperation in the Peaceful Uses of Outer Space (Jan. 13, 2010); Nima Nayebi, *The Geosynchronous Orbit and the Outer Limits of Westphalian Sovereignty*, 3 HASTINGS SCI. & TECH. L.J. 471, 477 n.33 (2011).

Since at least the 1980s, the international community has tried to create a single, comprehensive, and consensual framework for sustainable development.[27] Yet results so far have been mixed, both in terms of conceptual clarity and programmatic success. Some progress was made, though, in reviewing the five main principles coming out of the International Law Association's (ILA) New Delhi Declaration on Principles of International Law Relating to Sustainable Development, which included: integrated policy assessment, environmental sustainability, intergenerational equity, robust political participation, and intergenerational responsibility.[28] The ITU has also been integral in pushing the boundaries of the concept, especially as it is applied to ICT. For example, former ITU Secretary General Dr. Hamadoun I. Touré has stated of the connection between sustainability and cybersecurity that: "[o]ur common vision of the information society envisages safe, secure, and affordable access to global networks. It is a key component in ensuring social and economic progress and sustainable development for people in every corner of the world."[29] Aside from highlighting the positive vision of a sustainable cyber peace,[30] this quote also underscores the importance of cybersecurity itself in furthering the sustainability movement. Indeed, concepts from sustainability—from integrated reporting to certificate programs to leveraging the power of supply chains to spread positive network effects—have increasingly been applied to mitigating cyber risk.[31] This connection is further manifest in a myriad of ways, from making energy-intensive data centers more environmentally friendly[32] to bridging the often artificial divides between cybersecurity, and human rights such as privacy, and Internet governance. If this conceptualization is indeed accurate, then managing cyber attacks more effectively by instilling cybersecurity best practices while expanding Internet access and promoting human rights is vital to attaining the core tenants of sustainable development. At the firm level, this process is

27. *See* Douglas A. Kysar, *Sustainable Development and Private Global Governance*, 83 TEX. L. REV. 2109, 2115 (2005).

28. *See* The 70th Conference of the International Law Association (ILA), *ILA New Delhi Declaration on Principles of International Law Relating to Sustainable Development*, UN Doc. A/CONF.199/8 (Apr. 2, 2002), http://cisdl.org/tribunals/pdf/NewDelhiDeclaration.pdf.

29. MANAGING CYBER ATTACKS, *supra* note 9, at xiii.

30. For more on the distinction between negative and positive peace, see *id.* at xxv.

31. *See* Scott J. Shackelford & Timothy L. Fort, *Sustainable Cybersecurity: Applying Lessons from the Green Movement to Managing Cyber Attacks*, 2016 U. ILL. L. REV. 1995 (laying out the argument for applying concepts from the field of sustainable development to addressing an array of cybersecurity issues).

32. *See, e.g.*, Jen A. Miller, *How the Tech Industry is Greening its Data Centers*, CIO (Aug. 19, 2015, 6:27 AM), http://www.cio.com/article/2972935/data-center/how-the-tech-industry-is-greening-its-data-centers.html.

operationalized through Corporate Social Responsibility (CSR) to build, or if necessary rebuild, trust.[33] But in order for the full promise of both cyber peace and sustainable development to be realized, CSR should be married with the historically more top-down framework of international human rights law to help build a polycentric approach to promoting sustainable cybersecurity as is discussed further in Part IV.[34]

C. Introducing Polycentrism

Given the relative lack of binding black letter law in both the human rights and cybersecurity contexts, coupled with the active role played by governments and firms in each setting, it is important to move beyond stale approaches to regulation and recognize the dynamism possible by leveraging the power of polycentric governance. Sometimes called the Bloomington School of Political Economy, the "basic idea" of polycentric governance, according to Professor Michael McGinnis, is that a group facing a collective action problem "should be able to address" it in "whatever way they [the members of the group] best see fit."[35] This could include using existing governance structures or crafting new systems.[36] Polycentric governance regimes that are multi-level, multi-purpose, multi-type, and multi-sectoral in scope[37] could complement the top-down governance model favored throughout much of the history of human rights governance. Indeed, this polycentric model has already prevailed in the Internet governance context, which has enjoyed a more organic development trajectory.[38] Yet this trend is a

33. *See generally* Scott J. Shackelford, Timothy L. Fort & Jamie D. Prenkert, *How Businesses Can Promote Cyber Peace*, 36 U. PA. J. INT'L L. 353 (2015).

34. ANDREW W. MURRAY, THE REGULATION OF CYBERSPACE: CONTROL IN THE ONLINE ENVIRONMENT 47 (2007). For more on the role that polycentric governance can play in enhancing cybersecurity, see Scott J. Shackelford, *Toward Cyber Peace: Managing Cyber Attacks through Polycentric Governance*, 62 AM. U. L. REV. 1273 (2013).

35. Michael D. McGinnis, *Costs and Challenges of Polycentric Governance: An Equilibrium Concept and Examples from U.S. Health Care* 1 (The Vincent & Elinor Ostrom Workshop in Political Theory & Policy Analysis, Working Paper W11-3, 2011), http://php.indiana.edu/~mcginnis/Beijing_core.pdf.

36. *Id.* at 1–2.

37. *See* Michael D. McGinnis, *An Introduction to IAD and the Language of the Ostrom Workshop: A Simple Guide to a Complex Framework*, 39 POL'Y STUD. J. 169, 171 (2011) (defining "polycentricity" as "a system of governance in which authorities from overlapping jurisdictions (or centers of authority) interact to determine the conditions under which these authorities, as well as the citizens subject to these jurisdictional units, are authorized to act as well as the constraints put upon their activities for public purposes.").

38. *See, e.g.*, Scott J. Shackelford et al., *Back to the Future of Internet Governance?*, GEORGETOWN J. INT'L AFF. 81, 82 (2015).

double-edged sword with many nations seeking to assert greater control online, challenging the notion of cyberspace as a commons and fracturing governance at a time of increasing cyber insecurity.[39]

Indeed, polycentric governance is quickly coming into vogue as the preferred model of tackling "new" global collective action problems, marking a shift from more traditional twentieth century multilateral governance models. Increasingly, leaders across an array of fields, from the former President of Estonia, Toomas Ilves, and Director of the Internet Corporation for Assigned Names and Numbers (ICANN), Fadi Chehadé,[40] to Nobel Laureates such as Professor Elinor Ostrom, have proffered polycentric governance as the best path forward to addressing the global collective action problems of climate change and cyber attacks. Policymakers seem to be listening, as may be seen in the 2015 Paris Agreement at the 21st UN Framework Convention on Climate Change Conference of the Parties (COP21), which included a national pledge and review process that marked a departure point from previous multilateral attempts at climate negotiations.[41] This approach—which too has its faults, including a lack of hierarchy that can "yield gridlock rather than innovation"[42]—is also increasingly being tried in the human rights and cybersecurity contexts, as is discussed next in the context of the due diligence debate.

II. HUMAN RIGHTS DUE DILIGENCE PRIMER

Human rights law, as opposed to CSR, has traditionally been a multilateral response to the issue of fostering social responsibility in governments, and indirectly the businesses they regulate. That is, it is a top-down mechanism to achieve a desired end, but it is also one often without the power to bind stakeholders.[43] Many nations, for

---

39. *See* Elinor Ostrom, *A Polycentric Approach for Coping with Climate Change*, 32 (World Bank, Policy Research Working Paper No. 5095, 2010), http://elibrary.worldbank.org/doi/pdf/10.1596/1813-9450-5095.

40. *See* Nancy Scola, *ICANN Chief: "The Whole World is Watching" the U.S.'s Net Neutrality Debate*, WASH. POST (Oct. 7, 2014), https://www.washingtonpost.com/blogs/the-switch/wp/2014/10/07/internet-operations-chief-snowden-disclosures-make-my-job-easier/.

41. *See* David Victor, *Why Paris Worked: A Different Approach to Climate Diplomacy*, YALE ENV'T 360 (Dec. 15, 2015), http://e360.yale.edu/feature/why_paris_worked_a_different_approach_to_climate_diplomacy/2940/.

42. Robert O. Keohane & David G. Victor, *The Regime Complex for Climate Change*, 9 PERSP. ON POL. 7, 17 (2011), http://wws.princeton.edu/system/files/research/documents/KeohaneVictorFinal.pdf.

43. *See, e.g.*, Eric Posner, *The Case Against Human Rights*, GUARDIAN (Dec. 4, 2014, 1:00 PM), http://www.theguardian.com/news/2014/dec/04/-sp-case-against-human-rights. ("International human rights law reflects [a] . . . top-down mode of implementation. . . .").

example, engage in censorship practices that are in contravention of the Universal Declaration of Human Rights (UDHR), which includes Article 19's protections of freedom of speech, communication, and access to information.[44] This apparent disregard for the UDHR highlights the difficulty of relying on nonbinding international law to check the power of national governments and foster cyber peace, which further underscores the need for active private-sector engagement with more firms joining the thousands that have signed up to the UN Global Compact and the hundreds that have publicly stated policy positions on human rights.[45]

Facing pushback from nations weary of top-down approaches to fostering human rights protections, Special Representative of the UN Security-General John Ruggie crafted the Protect, Respect, and Remedy Framework (PRR Framework or Ruggie Framework) along with the accompanying Guiding Principles on Business and Human Rights (Guiding Principles) as a polycentric response to help move the ball forward.[46] First appointed as Special Representative of the Secretary-General on the issue of human rights and transnational corporations and other business enterprises in 2005, by 2008 the PRR Framework was ready for consideration by the Human Rights Council.[47] Rather than requiring the public and private sectors to change their behavior, the Guiding Principles offer voluntary frameworks and best practices that businesses can adapt to suit their own purposes. The thinking is that, if sufficient public pressure is brought, a standard of care may be indirectly created through this name-and-shame process, shaping corporate behavior in a perhaps more organic and politically palatable manner than traditional human rights treaties. So far, this approach has met with

---

44. *Internet censorship listed: how does each country compare?* GUARDIAN, https://www.theguardian.com/technology/datablog/2012/apr/16/internet-censorship-country-list (last visited Apr. 16, 2017); G.A. Res. 217 (III) A, Universal Declaration of Human Rights (Dec. 10, 1948) ("Everyone has the right to freedom of opinion and expression; this right includes the freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.").

45. *See* INST. FOR HUMAN RIGHTS & BUS., *supra* note 1, at 1.

46. *See, e.g.*, JOHN G. RUGGIE, supra note 5, at 78 ("The overriding lesson I drew . . . was that a new regulatory dynamic was required under which public and private governance systems . . . each come to add distinct value, compensate for one another's weaknesses, and play mutually reinforcing roles—out of which a more comprehensive and effective global regime might evolve, including specific legal measures. International relations scholars call this 'polycentric governance.'").

47. *See Understanding the Corporate Responsibility to Respect Human Rights*, HUM. RTS. & BUS. DILEMMAS F., http://hrbdf.org/understanding_business_responsibility/ (last visited Apr. 17, 2017).

some success, as shown by the regime's unanimous acceptance by the UN Human Rights Council in 2008 and again in 2011.[48]

The PRR Framework is built upon three pillars: (1) the State's duty to prevent and address corporate human rights abuse under international human rights law;[49] (2) the corporate responsibility to respect human rights, which exists independently from the first pillar;[50] and (3) access to judicial and non-judicial remedies in the event of a breach of one or both of the first two pillars.[51] Simply put, the "appropriate corporate response to managing the risks of infringing on the rights of others is to exercise human rights due diligence."[52] Indeed, the Guiding Principles have done a great deal to formalize the concept of human rights due diligence, which may be defined as: "An ongoing [and dynamic] risk management process . . . in order to identify, prevent, mitigate and account for how [a company] addresses its adverse human rights impacts. It includes four key steps: assessing actual and potential human rights impacts; integrating and acting on the findings; tracking responses; and communicating about how impacts are addressed."[53] These steps can, in turn, be simplified into three concrete and practical recommendations, which may be unpacked as: (1) implement a human rights policy, (2) relate it to human rights due diligence efforts, and (3) specify a remediation mechanism.[54] First, a firm's human rights policy should "be informed by appropriate internal and external expertise and identify what the company expects of its personnel and business partners. The policy should be approved at the most senior level and communicated internally and externally to all personnel, business partners and relevant stakeholders."[55] Second, regarding the operationalization of human rights due diligence,

48. *See, e.g.*, *UN Guiding Principles on Business and Human Rights*, SHIFT PROJECT, http://www.shiftproject.org/page/un-guiding-principles-business-and-human-rights (last visited Apr. 16, 2017).

49. *Id.*

50. *Id.*

51. U.N. Human Rights Council, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, U.N. Doc. A/HRC/17/31, at 22 (Mar. 21, 2011), http://www.ohchr.org/Documents/Issues/Business/A-HRC-17-31_AEV.pdf.

52. *Understanding the Corporate Responsibility*, *supra* note 47.

53. *Human Rights Due Diligence*, *supra* note 4.

54. *Id.*

55. *Understanding the Corporate Responsibility to Respect Human Rights*, *supra* note 47. Moreover, beyond drafting and updating the policy itself, it is important for firms that: "all internationally-recogni[z]ed human rights are understood as being relevant; that clear responsibilities are established specifying who within the company is accountable for overall human rights policy; that the most relevant functional areas and existing policies are identified; that the company's human rights reporting commitments are well-defined; and that

firms should, at a minimum, commit to periodic assessments as to the "actual and potential human rights impacts of company activities and relationships," then integrate these commitments into "internal control and oversight systems," track corporate performance on a regular basis, and provide public and regular reporting on performance.[56] Finally, if adverse impacts occur, firms should "cooperate in their remediation through legitimate processes,"[57] such as through engaging third party consultancies, civil society groups, and, if necessary, outside counsel.

Despite the clarity brought by these steps, there remains no standard way of conducting human rights due diligence; "businesses are very diverse and they must decide what is best suited for them."[58] Regardless of the type and rate of corporate implementation, the most proactive firms recognize that due diligence is "not a one-time thing[,] but an ongoing process."[59] As European policymakers have stated,

> Human rights due diligence should start at the earliest pre-contract stages of a project's lifecycle and continue through operations, to the project's decommissioning and post-closure stages. It is about on-going processes, not one-off events such as an impact assessment at the start of a new project, or an annual report.[60]

Guides have also been created by civil society to aid firms in creating their own human rights policies, which include suggestions that all policies, at a minimum, require: (1) "An explicit commitment to respect all human rights which refers to international human rights

---

conflicts between local practice or law and international human rights standards are understood and are being proactively managed." INST. FOR HUMAN RIGHTS & BUS., *supra* note 1, at 2.

56. INST. FOR HUMAN RIGHTS & BUS., *supra* note 1, at 7. It is also vital that firms take a more proactive stance, such as by "reinforcing human rights in business culture[s][,] . . . [which could] include raising rights awareness through training and emphasizing the importance of human rights due diligence within recruitment, hiring, training and appraisal processes, besides developing clear incentives and disincentives to encourage good performance and discourage bad behavior with regard to human rights." *Id.* at 2.

57. U.N. Human Rights Council, *supra* note 51, at 24.

58. ECONSENSE, RESPECTING HUMAN RIGHTS: TOOLS AND GUIDANCE MATERIALS FOR BUSINESS 8 (2014), http://www.econsense.de/sites/all/files/Respecting_Human_Rights.pdf; *see also* INST. FOR HUMAN RIGHTS & BUS., *supra* note 1, at 2 (arguing that "more transparency is needed on 'impact' or 'outcome' indicators to supplement many of the more 'process-oriented' approaches to human rights reporting currently under development.").

59. ECONSENSE, *supra* note 58, at 8.

60. EUROPEAN COMM'N, OIL AND GAS SECTOR GUIDE ON IMPLEMENTING THE UN GUIDING PRINCIPLES ON BUSINESS & HUMAN RIGHTS 14 (2013).

standards, including the UDHR; (2) discussion of labor and employee rights; (3) provisions for non-labor rights reflecting a particular industry or sector's environment; and (4) a commitment for companies to act in accordance with their policy goals."[61]

Beyond corporations, and reflecting the State's duty to promote human rights under the Guiding Principles along with firms, the concept of human rights due diligence has also been increasingly codified by nations, including the United States, such as under the conflict minerals provisions of the Dodd-Frank Wall Street Reform and Consumer Protection Act, which require that companies must provide "a description of the measures taken . . . to exercise due diligence on the source and chain of custody of minerals."[62] This due diligence process must comport with a nationally or internationally recognized relevant framework,[63] and should reflect a "know-and-show" style of due diligence, along with auditing and reporting in accordance with the Guiding Principles and Professor Ruggie's broader vision of human rights due diligence norm.[64] In particular, Section 1502 of Dodd-Frank is likely evidence that human rights due diligence has entered the "norm cascade" phase of the norm life cycle in international relations in which rules of the road become widely disseminated,[65] despite some continued controversy.[66] However, the election of Donald Trump and his promise to "dismantle Dodd-Frank" could cast doubt on this conclusion in the U.S. context post-2016.[67] Regardless, this regime has had an important influence on a global norm creation that would survive the statute's revision or repeal.

---

61. ECONSENSE, *supra* note 58, at 10.

62. Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, Pub. L. No. 111–203, 124 Stat. 1376, 2213 (codified at 15 U.S.C. § 78m(p)(1)(A)(i) (2012)).

63. Conflict Minerals, 77 Fed. Reg at 56,326; *see* Prenkert & Shackelford, *supra* note 3, at 475–79.

64. *See* U.N. Human Rights Council, *supra* note 51.

65. *See* JOHN G. RUGGIE, supra note 5, at 128–29 (citing Martha Finnemore & Kathryn Sikink, *International Norm Dynamics and Political Change*, 52 INT'L ORG. 887 (1998)) (describing the life-cycle of norm uptake). In contrast, the relative paucity of national or internationally recognized due diligence frameworks that can be used by companies to comply with the SEC rule and the resistance that business groups have exhibited to the due diligence requirement are both evidence that the human rights due diligence norm has not advanced to the internalization stage, where the norm takes on a taken-for-granted quality. *See id.* (describing norm internalization). For a thorough analysis of Section 1502, see Galit A. Sarfaty, *Human Rights Meets Securities Regulation*, 54 VIRG. J. INT'L L. 97 (2013).

66. *See* Sarfaty, *supra* note 65, at 98 n.6 (noting the lawsuits filed by the U.S. Chamber of Commerce, Business Roundtable, and industry groups to nullify SEC rules designed to operationalize Section 1502).

67. Jesse Hamilton & Elizabeth Dexheimer, *Trump's Transition Team Pledges to Dismantle Dodd-Frank Act*, BLOOMBERG (Nov. 10, 2016, 3:38 PM), http://www.bloomberg.com/news/articles/2016-11-10/trump-s-transition-team-pledges-to-dismantle-dodd-frank-act.

Beyond nations, other governance levels from local to global are taking action on human rights due diligence—including cities, such as Pittsburgh, Pennsylvania; St. Petersburg, Florida; and Edina, Minnesota, which have passed resolutions calling on local firms to promote human rights due diligence.[68] A number of organizations have also imparted to their stakeholders education and guidance meant to provide additional support for and uptake of the human rights due diligence norm. An example of such private stakeholder human rights governance initiatives is the IPC–Association Connecting Electronics Industries, which has promulgated Conflict Minerals Due Diligence Guidance.[69] Similarly, in keeping with the multi-level approach to due diligence envisioned under the polycentric Ruggie Guiding Principles, the OECD adopted the Due Diligence Guidance for Responsible Supply Chains of Minerals from Conflict-Affected and High-Risk Areas (Due Diligence Guidance) in May 2011.[70] This stands in marked contrast to the political resistance to more top-down human rights formulations, including in the context of supply chains.[71] Together, these examples highlight the fact that human rights due diligence is an increasingly prominent—if still somewhat underdeveloped[72]—shaper of corporate behavior across numerous stakeholders. Until recently, however, the link between human rights and related areas including cybersecurity was underappreciated. We turn to that task

---

68. Joe DiLeo & Tim Kolber, *As Good as Gold? SEC Issues Final Rule on Conflict Minerals*, 19 DELOITTE HEADS UP, Sept. 11, 2012, at app. D, https://www.iasplus.com/en/publications/us/heads-up/2012/heads-up-2014-sec-issues-final-rule-on-conflict-minerals/file.

69. Press Release, Assoc. Connecting Electronics Indus., New IPC Guide Spells out Electronics Manufacturers' Conflict Minerals Due Diligence Obligations, (Feb 12, 2013), http://www.ipc.org/ContentPage.aspx?pageid=new-IPC-Guide-Spells-Out-Electronics-Manufacturers-Conflict-Minerals-Due-Diligence-Obligations; s*ee* Mark B. Taylor, *The Ruggie Framework: Polycentric Regulation and the Implications for Corporate Social Responsibility*, 5 NORDIC J. APPLIED ETHICS 9, 23–25 (2011) (discussing how the Ruggie idea of due diligence and reporting "knowing and showing" has been incorporated in the approach to conflict minerals).

70. OECD DUE DILIGENCE GUIDANCE FOR RESPONSIBLE SUPPLY CHAINS OF MINERALS FROM CONFLICT-AFFECTED AND HIGH-RISK AREAS 3 (2d ed. 2013), http://www.oecd.org/daf/inv/mne/GuidanceEdition2.pdf.

71. *Cf.* Sabrina Basran, *The Impact of Ruggie's Guiding Principles for Human Rights?*, CSR INT'L (Mar. 26, 2012), http://csrinternational.blogspot.com/2012/03/impact-of-ruggies-guiding-principles.html ("A year on, what impact has Ruggie's Framework (particularly the second pillar) had on business behaviour? Not much. Beyond a stated commitment to the Guiding Principles in a few CSR reports and Code of Ethics, there has been a conspicuous lack of activity by companies in implementing the Framework. This is not to say there has been none, but examples are few and far between.").

72. *See* Sarfaty, *supra* note 65, at 106 ("Critics have argued, however, that this approach limits human rights disclosure to material impacts—that is, those impacts that may cause legal, reputational, or other business risks—and that reporting may not lead to changes in corporate behavior.").

next before discussing how these concepts may be married together under the umbrella of sustainable development in Part IV.

III. UNPACKING CYBERSECURITY DUE DILIGENCE

What is cybersecurity due diligence, and how is it similar to, or distinct from, conceptions of human rights due diligence? In the private-sector transactional context, cybersecurity due diligence has been defined as: "the review of the governance, processes and controls that are used to secure information assets."[73] This increasingly central concept to a variety of business activities as it is used here builds from this definition and may be understood as the corporate, national, and international obligations of both State and non-State actors to help identify and instill cybersecurity best practices and effective governance mechanisms so as to promote cyber peace by enhancing the security ICT infrastructure and the entrenchment of human rights. Put more simply, due diligence refers to activities used to identify and understand the various risks facing your organization. Cybersecurity due diligence, then, is centered on risk management best practices and obligations that may exist between States, between non-State actors (e.g., private corporations, end-users), and between State and non-State actors,[74] and refers to the international obligations of both State and non-State actors to help identify and instill cybersecurity best practices so as to promote the security of critical ICT infrastructure. In so doing, the norm "commits states to ensuring that no actions originating on their territory in times of peace violate the rights of other states."[75] But determining exactly what nations' due diligence obligations are to secure their networks and to prosecute or extradite cyber attackers is no simple matter. Yet surprisingly, given the concept's increasing centrality, it has received relatively little attention in the literature.[76]

---

73. *Cyber Due Diligence: Pre-Transaction Assessments Can Uncover Costly Risks,* KROLL CALL (Jan. 28, 2015), http://blog.kroll.com/2015/cyber-due-diligence-pre-transaction-assessments-can-uncover-costly-risks/.

74. An earlier version of this research was previously published as Shackelford, Russell, & Kuehn, *supra* note 6, at 4.

75. Annegret Bendiek, Due Diligence in Cyberspace: Guidelines for International and European Cyber Policy and Cybersecurity Policy 7 (Stiftung Wissenschaft und Politik Research Paper, 2016), http://www.swp-berlin.org/fileadmin/contents/products/research_papers/2016RP07_bdk.pdf.

76. *Cf. White House and Department of Defense Announce Strategies to Promote Cybersecurity*, 105 AM. J. INT'L L. 794, 795 (2011) ("Cybersecurity Due Diligence: States should recognize and act on their responsibility to protect information infrastructures and secure national systems from damage or misuse."); John M. Prescott, *Responses to Five Questions on National Security Law*, 38 WM. MITCHELL L. REV. 1536, 1541 (2012) (discussing the U.S. International Strategy

This subsection briefly reviews the relevant international law and discusses how a small subset of companies and countries—namely the United States and Germany—are operationalizing the concept, before moving on to discuss areas of convergence with the literature on human rights due diligence.

The international law on cybersecurity due diligence remains somewhat ambiguous, though there have been helpful steps forward as may be seen in the *Tallinn* projects and related undertakings.[77] Precedent from the International Court of Justice (ICJ), for example, must be analogized from different contexts, and is to a certain extent contradictory. For instance, the Court held in *Corfu Channel* that it is "every State's obligation not to allow knowingly its territory to be used for acts contrary to the rights of other States."[78] As applied to cybersecurity, this decision could implicate a duty to warn other States as to vulnerabilities in its networks that could be exploited by malicious actors and used to harm other nations.[79] There is some support for this understanding as part of the 2015 G20 communique that called for a "duty to assist" victim nations,[80] which could implicitly include a duty to warn these nations of impending cyber attacks. Similarly, the ICJ held in *Trail Smelter* (involving a 1935 transboundary air pollution dispute between the

---

for Cyberspace); Scott J. Shackelford, *Toward Cyberpeace: Managing Cyber Attacks through Polycentric Governance*, 62 AM. U. L. REV. 1273, 1354 (2013) (discussing the due diligence aspect of the 2011 U.S. International Strategy for Cyberspace).

77. *See, e.g.*, *Tallinn Manual 2.0 to be Completed in 2016*, NATO COOPERATIVE CYBER DEF. CEN. EXCELLENCE (Oct. 9, 2015), https://ccdcoe.org/tallinn-manual-20-be-completed-2016.html; *see also* Shackelford, Russell, & Kuehn, *supra* note 6; Shackelford & Russell, *supra* note 6.

78. Corfu Channel (U.K. v. Albania), 1949 I.C.J. 4, 22 (Apr. 9), http://www.icj-cij.org/docket/files/1/1645.pdf.

79. *See* Eneken Tikk, *Ten Rules for Cyber Security*, 53 SURVIVAL 119, 119 (2011).

80. *See* Communiqué, G20, G20 Leaders' Communiqué agreed in Antalya: Antalya (Nov. 15–16, 2015), http://g20.org.tr/g20-leaders-commenced-the-antalya-summit. ("In the ICT environment, just as elsewhere, states have a special responsibility to promote security, stability, and economic ties with other nations. In support of that objective, we affirm that no country should conduct or support ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sectors. All states in ensuring the secure use of ICTs, should respect and protect the principles of freedom from unlawful and arbitrary interference of privacy, including in the context of digital communications. We also note the key role played by the United Nations in developing norms and in this context we welcome the 2015 report of the UN Group of Governmental Experts in the Field of Information and Telecommunications in the Context of International Security, affirm that international law, and in particular the UN Charter, is applicable to state conduct in the use of ICTs and commit ourselves to the view that all states should abide by norms of responsible state behavior in the use of ICTs in accordance with UN resolution A/C.1/70/L.45. We are committed to help ensure an environment in which all actors are able to enjoy the benefits of secure use of ICTs.").

U.S. and Canada and representing the first application of the "polluter pays" principle in international law) that "no State has the right to use or permit the use of its territory . . . to cause injury by fumes . . . to the territory of another . . . when the case is of serious consequence and the injury is established by clear and convincing evidence."[81] Even though the decision was directed towards the emission of "fumes," *Trail Smelter* has come to represent the broader "no harm" principle, which requires of States "that activities within their jurisdiction or control respect the environment of other States."[82] This "no harm" principle, although directed towards the environment, enjoys parallels with cybersecurity, and may serve as the foundation for a broader State obligation not to permit domestic activities that result in serious international consequences. However, the Court's *Nicaragua* decision, in which it held that nations have an obligation not to interfere in one another's domestic affairs if that intervention relates to "the choice of a political, economic, social, and cultural system, and the formulation of foreign policy,"[83] may be read as being in contradiction to the Court's effects jurisdiction analysis in *Trail Smelter*. This latter case also tracks the divergent State practice on Internet governance with some States asserting varying degrees of Internet sovereignty while others profess internet freedom and the virtues of the "global networked commons."[84] In summary, the ICJ jurisprudence is unsettled and is far from dispositive on the question of a cybersecurity due diligence norm.

As such, both State practice as well as lessons from the private sector can and should be considered to help build out a comprehensive approach to due diligence. Space constraints prohibit a thorough exploration of these topics,[85] but in brief, more nations are discussing the importance of cybersecurity due diligence, including as part of their national cybersecurity strategies. The U.S. government, for example, has created the NIST Cybersecurity Framework, introduced above.[86] This is important for a variety of

81. Trail Smelter Arbitration (U.S. v. Can.), 3 R.I.A.A. 1905, 1965 (1941).

82. Ralph Bodle, *Climate Law and Geoengineering*, *in* CLIMATE CHANGE AND THE LAW 447, 457 (Erkki Hollo et al. eds., 2012).

83. Case Concerning the Military and Paramilitary Activities in and Against Nicaragua (Nicar. v. U.S.), Judgment, 1986 I.C.J. 14, 106–08, 183 (June 27).

84. Hillary Rodham Clinton, U.S. Sec'y of State, Remarks on Internet Freedom (Jan. 21, 2010) *in Clinton's Speech on Internet Freedom, January 2010*, COUNCIL ON FOREIGN REL. (Jan. 21, 2010) http://www.cfr.org/internet-policy/clintons-speech-internet-freedom-january-2010/p21253.

85. For more, see Shackelford, Russell, & Kuehn, *supra* note 6; Shackelford & Russell, *supra* note 6.

86. *See supra* note 11.

reasons, including its roll in clarifying a standard of cybersecurity care in the U.S. that directly plays into the topic of due diligence.[87] For example, although the NIST Framework was only published in 2014, some private-sector clients are already receiving the advice that if their "cybersecurity practices were ever questioned during litigation or a regulatory investigation, the 'standard' for 'due diligence' was now the NIST Cybersecurity Framework."[88] Eventually, the NIST Framework holds the potential not only to shape a standard of care for domestic critical infrastructure organizations, but also could help to harmonize global cybersecurity best practices for the private sector writ large given active NIST collaborations with several dozen nations including the United Kingdom, Japan, Korea, Estonia, Israel, and Germany.[89]

Germany's cybersecurity due diligence efforts are world-leading in many respects and rely in particular on close collaboration between the public and private sectors, nationally and globally.[90] Long known for its robust national data protection laws, Germany is now moving to create strict cybersecurity standards for critical infrastructure as part of a broader approach to developing the field of cybersecurity due diligence.[91] For example, SWP, a leading German defense think tank, issued a report on cybersecurity due diligence in 2016 in which it encouraged the development of a cybersecurity

87. For more information on the NIST Cybersecurity Framework, see Scott J. Shackelford et al., *Toward a Global Cybersecurity Standard of Care?: Exploring the Implications of the 2014 Cybersecurity Framework on Shaping Reasonable National and International Cybersecurity Practices*, 50 TEX. INT'L L.J. 303 (2015).

88. John Verry, *Why the NIST Cybersecurity Framework Isn't Really Voluntary*, INFO. SEC. BLOG (Feb. 25, 2014), http://www.pivotpointsecurity.com/risky-business/nist-cybersecurity-framework.

89. There is some evidence that this may already be happening, including with regards to the Federal Trade Commission's cybersecurity enforcement powers. *See, e.g.*, Brian Fung, *A Court Just Made it Easier for the Government to Sue Companies for Getting Hacked*, WASH. POST (Aug. 24, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/08/24/a-court-just-made-it-easier-for-the-government-to-sue-companies-for-getting-hacked/?wpmm=1&wpisrc=NL_headlines. For more on this topic, see Scott J. Shackelford, Scott Russell, & Jeffrey Haut, *Bottoms Up: A Comparison of "Voluntary" Cybersecurity Frameworks*, 16 U.C. DAVIS BUS. L.J. 217 (2016).

90. *See* BUNDESMINISTERIUM DES INNERN [FED. MINISTRY OF THE INTERIOR], CYBER-SICHERHEITSSTRATEGIE FÜR DEUTSCHLAND [CYBERSECURITY STRATEGY FOR GERMANY] (2016), https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf.

91. *See* BUNDESMINISTERIUM DES INNERN [FED. MINISTRY OF THE INTERIOR], SCHUTZ KRITISCHER INFRASTRUKTUREN—RISIKO—UND KRISENMANAGEMENT: LEITFADEN FÜR UNTERNEHMEN UND BEHÖRDEN [PROTECTION OF CRITICAL INFRASTRUCTURES—RISK AND CRISIS MANAGMENT: GUIDELINES FOR COMPANIES AND AUTHORITIES] (2011), http://www.bbk.bund.de/SharedDocs/Downloads/BBK/DE/Publikationen/PublikationenKritis/Leitfaden_Schutz-Kritis.pdf?__blob=publicationFile.

due diligence norm as part of Germany's 2016 national cybersecurity strategy.[92] In describing its conception of due diligence, SWP argues that the norm builds from "the international legal standard of due diligence, which stipulates that a state must do everything necessary to prevent actions emanating from within its own territory that might infringe the rights of third parties[,]"[93] which in turn echoes the ICJ's holding in *Trail Smelter* as well as the OECD's work on due diligence.[94] This emerging norm is playing out in Germany and across Europe in numerous ways, including deeper public-private cooperation (as seen in the new Network and Information Security (NIS) Directive requiring all EU Member States to promulgate "minimum standards and reporting requirements for IT security, and operators of critical infrastructure must be involved in fighting cyber- crime,")[95] and the inclusion of more stakeholders in the policy formation process.[96] More broadly, there is also an interrelationship between due diligence and Internet governance to consider, in particular the continuation of a multistakeholder (e.g., including both public- and private-sector organizations), as opposed to a multilateral (state-on-state), approach to regulating cyberspace.[97] Debate persists about the extent to which a cybersecurity due diligence norm—as with human rights—should be enforceable on public- and private-sector stakeholders, and if so, at what level of governance is it most appropriate to exercise oversight.[98]

An analysis of how these cyber powers approach cybersecurity due diligence only moves the discussion so far though, given that many of the most innovative best practices come not from nations, but the private sector,[99] which has had to respond to a rash of cybersecurity threats. Jason Weinstein, former Deputy Assistant Attorney

92. Bendiek, *supra* note 75, at 5.

93. *Id.*

94. *Id.*

95. *Id.* at 6.

96. *Id.*

97. *Id.*; *see also* Scott J. Shackelford, *The Coming Age of Internet Sovereignty?*, *in* INTERNET CENSORSHIP (Margaret Haerens & Lynn M. Zott eds., 2014) (discussing the risk of Internet fragmentation); Scott J. Shackelford et al., *Back to the Future of Internet Governance?*, GEO. J. INT'L AFF. (June 25, 2015) (analyzing the trajectory of Internet governance through the lens of the leading cyber powers).

98. *See* Bendiek, *supra* note 75, at 6 (arguing for "arbitration authorities" being given oversight "to ensure that due diligence is properly implemented.").

99. *See id.* at 15 (discussing the extent to which the German IT sector is helping to developing cybersecurity due diligence standards). For a list of the cyber powers, see BOOZ ALLEN HAMILTON, CYBER POWER INDEX: FINDINGS AND METHODOLOGY https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/EIU%20-%20Cyber%20Power%20Index%20Findings%20and%20Methodology.pdf.

General at the U.S. Department of Justice, summarized the issue of cybersecurity due diligence succinctly when he said: "When you buy a company, you're buying their data, and you could be buying their data-security problems."[100] In other words, "[c]yber risk should be considered right along with financial and legal due diligence considerations."[101] A majority of respondents to one 2014 survey reported that cybersecurity challenges are already altering the M&A landscape,[102] leading the American Bar Association to release a cybersecurity checklist for contracting parties that features due diligence.[103] In other words, despite growing recognition as to the scale and scope of the multifaceted cyber threat facing firms, many remain predominantly reactive,[104] and are thinking of due diligence too narrowly, artificially putting up barriers between human rights and cybersecurity that arguably do not belong and are not helpful.

IV. LINKING HUMAN RIGHTS AND CYBERSECURITY UNDER SUSTAINABLE DEVELOPMENT

As has been discussed in Parts III and IV, due diligence is an important concept permitting both countries and companies to better understand and meet their risk management goals. This process is playing out through operationalizing the no-harm principle, by which more firms are using the Guiding Principles to instill human rights best practices in their decision making, along with the NIST Cybersecurity Framework, to help guide cybersecurity investments.[105] Similarly, countries are operationalizing these concepts through domestic statutes ranging from Section 1502 of

---

100. Rachel Ensign, *Cybersecurity Due Diligence Key in M&A Deals*, WALL ST. J.: RISK AND COMPLIANCE BLOG (Apr. 24, 2014, 1:50 PM), http://blogs.wsj.com/riskandcompliance/2014/04/24/cybersecurity-due-diligence-key-in-ma-deals.

101. Erin Ayers, *Cybersecurity Easing its way into M&A Due Diligence*, CYBER RISK NETWORK (Aug. 22, 2014), http://www.cyberrisknetwork.com/2014/08/22/cybersecurity-easing-way-ma-process/. [this link could not be found on my laptop]

102. *Id.*

103. *See* A.B.A. Cybersecurity Legal Task Force, VENDOR CONTRACTING PARTY: CYBERSECURITY CHECKLIST (2016), http://www.americanbar.org/content/dam/aba/images/law_national_security/Cybersecurity%20Task%20Force%20Vendor%20Contracting%20Checklist%20v%201%2010-17-2016%20cmb%20edits%20clean.pdf.

104. *See* MCAFEE, UNSECURED ECONOMIES: PROTECTING VITAL INFORMATION 6 (2009), https://www.cerias.purdue.edu/assets/pdf/mfe_unsec_econ_pr_rpt_fnl_online_012109.pdf (comparing cybersecurity investment rates across countries and concluding that "[i]t appears that decision makers in many countries, particularly developed ones, are reactive rather than proactive.").

105. *See* Ilse Griek, *UN Forum on Human Rights: Assessing the Ruggie Framework*, SUSTAINALYTICS, http://www.sustainalytics.com/assessing-ruggie-framework (last visited Sept. 12, 2016).

Dodd Frank, the Cybersecurity Act of 2015, to the EU NIS Directive. However, these dual arenas of due diligence—comprising human rights and cybersecurity—remain largely separate as matters of corporate decision making and public policymaking, despite a growing recognition by intergovernmental organizations and civil society that both of these concepts are vital components of sustainable development.[106] This may be seen explicitly in the 2015 Sustainable Development Goals, which state that "universal and affordable access to ICTs" is vital in twenty-first century sustainable development, but that this will not be possible without building confidence and security across ICTs.[107] This final Part explores these linkages and how they mesh with the growing literature on polycentric governance, ultimately arguing for a bottom-up, comprehensive approach to enterprise risk management.

Human rights due diligence, as embodied in the Ruggie Guiding Principles discussed in Part II, calls for developing corporate policies, assessing the impacts of corporate actions, integration, as well as tracking and monitoring performance such that actions mesh well with stated goals as part of an overarching goal of mitigating harm to other stakeholders. State action is considered—indeed, required under international human rights law—to ensure that corporations take the necessary steps, as we have begun to see in the United States, along with the availability of judicial and nonjudicial remedies in the event of a breach.[108] Similarly, cybersecurity due diligence is emerging under international law as a mechanism "to hold states to account for omissions in making their infrastructure safe; for breaching their obligations by neglecting to take action; or for a lack of cooperation in protecting against and solving cyber attacks."[109] Such sentiments have been backed up by action at multiple governance levels above and beyond the national and regional examples discussed above. For example, in 2000, the UN General Assembly called upon states, "[to] ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies."[110] The UN Group of Governmental Experts (GGE) picked up this idea in its final report of June

106. *See* INT'L TELECOMM. UNION, *supra* note 7.

107. *Id.*

108. *See UN Guiding Principles on Business and Human Rights*, *supra* note 48.

109. Christian Schaller, Internationale Sicherheit und Voülkerrecht im Cyberspace [International Security and International Law in Cyberspace] 25 Stiftung Wissenschaft und Politik Research Paper, 2014).

110. Bendiek, *supra* note 75, at 8 (quoting United Nations Resolution on Combating the Criminal Misuse of Information Technologies, G.A. Res. 55/63, at 2 (Dec. 4, 2000), http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_55_63.pdf).

2015, which encourages all states to "ensure that their territories, and especially the computer systems and infrastructure situated there or otherwise under the states' control, is not misused for attacks on the infrastructure of other states."[111] In other words, States are increasingly expected by the international community to work "in cooperation with other states . . . to do everything that may be reasonably expected of them to help deliver an 'open, free and secure Internet.'"[112] This requires domestic policies with, according to SWP, a high level of representativity, inclusiveness, and transparency,[113] mirroring calls for a more robust human rights due diligence regime. Indeed, the argument has been made that, to be truly effective, firms exercising human rights due diligence should perhaps go beyond the Ruggie Framework and include requirements of transparency, external participation and verification, as well as continuous monitoring and review in order to meet their human rights goals.[114] These common notions of diverse representation, inclusiveness, transparency, verification, and effective dispute resolution, in turn, mirror both the overriding goals of sustainable development—in particular the "no harm" principle introduced in Part I(B), which also is integral to discussions of human rights and cybersecurity due diligence—and polycentric governance.

Beginning in the early 1990s with her groundbreaking book *Governing the Commons*, Professor Elinor Ostrom created an informative framework of eight design principles for the management of common pool resources known as the Ostrom design principles, which has come to represent some of the core features of successful polycentric systems.[115] These principles include the importance of: (1) "clearly defined boundaries for the user pool . . . and the resource domain";[116] (2) "proportional equivalence between benefits and costs";[117] (3) "collective choice arrangements" ensuring "that the resource users participate in setting . . . rules";[118] (4) "monitoring . . . by the appropriators or by their agents";[119] (5) "graduated

111. Bendiek, *supra* note 75, at 8.

112. *Id.*

113. *Id.*

114. *See* James Harrison, An Evaluation of the Institutionalisation of Corporate Human Rights Due Diligence (2012) Warwick School of Law Research Paper 2012/18, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2117924.

115. *See* ELINOR OSTROM, GOVERNING THE COMMONS: THE EVOLUTION OF INSTITUTIONS FOR COLLECTIVE ACTION 212 (1990).

116. SUSAN J. BUCK, THE GLOBAL COMMONS: AN INTRODUCTION 32 (1998).

117. *See* OSTROM, *supra* note 115, at 90.

118. BUCK, *supra* note 116, at 32.

119. *Id.*

sanctions" for rule violators";[120] (6) "conflict-resolution mechanisms [that] are readily available, low cost, and legitimate";[121] (7) "minimal recognition of rights to organize";[122] and (8) "governance activities [being] . . . organized in multiple layers of nested enterprises."[123] Not all of Professor Ostrom's design principles are applicable in either the context of human rights or cybersecurity, and space constraints prohibit a deep analysis here.[124] However, the overlap between many of these principles—including diverse representation, monitoring, and effective dispute resolution mechanisms—with efforts to refine and build out the sustainable development due diligence norm is apparent.

The fields of cybersecurity and human rights due diligence are further coming together explicitly surrounding issues of civil rights and data protection.[125] This convergence may be seen in such areas as the Internet freedom and net neutrality movement regarding the free flow of information and ideas across borders, which is part and parcel of the multi-stakeholder approach to Internet governance discussed in Part III.[126] A key question for Internet governance going forward is how best to assure "the availability, confidentiality, authenticity[,] and integrity of data[,]"[127] as well as, more broadly, how best to reinforce human rights best practices across stakeholders—including, but not limited to, private users, civil society, academia, and the public and private sectors—as part of the overarching debate on Internet governance and informational self-determination.[128] It is vital to foster the active engagement of diverse stakeholders, including representative civil society interests, in

120. *Id.*

121. *Id.*

122. Elinor Ostrom, *Polycentric Systems: Multilevel Governance Involving a Diversity of Organizations*, *in* GLOBAL ENVIRONMENTAL COMMONS: ANALYTICAL AND POLITICAL CHALLENGES INVOLVING A DIVERSITY OF ORGANIZATIONS 105, 118 tbl. 5.3 (Eric Brousseau et al. eds., 2012) (noting that polycentric systems frequently enjoyed better outcomes than those of central governments).

123. *Id.*

124. *See* Prenkert & Shackelford, *supra* note 3; in MANAGING CYBER ATTACKS, *supra* note 9, at Ch. 2.

125. *See* Bendiek, *supra* note 75, at 19.

126. *See id.* at 22; s*ee also* Madeline Carr, *Power Plays in Global Internet Governance*, 43 MILLENNIUM J. OF INT'L STUD. 640 (2014) (arguing for a more balanced approached to studying the benefits and drawbacks of multi-stakeholder Internet governance, including its capacity to reinforce existing (potentially skewed) power dynamics).

127. Bendiek, *supra* note 75, at 22. One manifestation of this trend is the debate over "fake news" and its mitigation. *See, e.g.*, Peter Kafka, *Facebook Has Started to Flag Fake News Stories*, RECODE (Mar. 4, 2017, 6:22 PM), http://www.recode.net/2017/3/4/14816254/facebook-fake-news-disputed-trump-snopes-politifact-seattle-tribune .

128. *See* Bendiek, *supra* note 75, at 22; *see also* Scott J. Shackelford, *Should Cybersecurity Be a Human Right?*, CONVERSATION (Feb. 13, 2017, 9:15 PM), http://theconversation.com/should-

order for effective progress to be made in this context, and for the promise of multi-stakeholder Internet governance more generally to be realized in keeping with the core principles of both sustainable development and polycentric governance.[129]

The convergence of human rights, cybersecurity, and Internet governance more generally has also begun to be codified, such as may be seen by the UN Human Rights Council's 2012 resolution that human rights are equally valid online and offline.[130] Since this resolution, the debate has moved on to topics like encryption, with the "UN's special rapporteur on freedom of expression, David Kaye, call[ing] for the encryption of private communications to be made a standard."[131] International data flows, including those from the European Union to the United States, and vice versa, also continue to be a hot topic with the fall of the Safe Harbor regime and the rise of the Privacy Shield.[132] Another overarching concern is the appropriate role for, and degree of, cybersecurity regulation being imposed by countries. SWP argues, for example, that "States should only intervene in a regulatory capacity when self-regulation can no longer guarantee democratic legitimacy, effectiveness, rule of law and transparency."[133] This perspective, in turn, resonates with the findings of the polycentric governance literature, which warns against "crowding out" smaller-scale efforts,[134] such as the experimentation surrounding due diligence being undertaken by firms, cities, countries, and regions discussed throughout this Article.

CONCLUSION

From 2010–15, the Institute for Human Rights and Business argued that the overriding goals with regards to human rights due diligence should be broadly interpreted to achieve growth and

---

cybersecurity-be-a-human-right-72342 (discussing the extent to which Internet access and cybersecurity are emerging human rights).

129. *See, e.g.*, Carr, *supra* note 126, at 657; Stuart N. Brotman, *Multistakeholder Internet Governance: A Pathway Completed, the Road Ahead.* CTR. FOR TECH. INNOVATION AT BROOKINGS (July 2015) https://www.brookings.edu/wp-content/uploads/2016/06/multistakeholder.pdf.

130. *Id.*; Human Rights Council Res. 20, U.N. Doc. A/HRC/20/L.13 (June 29, 2012), http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A.HRC.20.L.13_en.doc.

131. Bendiek, *supra* note 75, at 19.

132. For more on this topic, see Scott J. Shackelford, Seeking a Safe Harbor in a Widening Sea: Unpacking the EJC's Schrems Decision and What it Means for Transatlantic Relations (Oct. 26, 2015) (unpublished manuscript) (on file with author).

133. Bendiek, *supra* note 75, at 23.

134. *See, e.g.*, Elinor Ostrom, *Beyond Markets and States: Polycentric Governance of Complex Economic Systems*, 100 AM. ECON. REV. 641, 656 (2010).

deepen understanding.[135] More specifically, the Institute identified five themes in need of greater attention: "(1) Developing human-centered approach to business management; (2) establishing clarity about the explicit use of human rights terminology, standards and language; (3) integrating human rights in contractual relationships; (4) setting up accountability and grievance-mechanisms; and (5) ensuring transparency."[136] In many ways, the challenge from 2016–21 remains the same, except to add to this list the need to incorporate cybersecurity within firms' human rights due diligence operations as part of a broader conceptualization of how corporate operations are impacting sustainable development and avoiding harm to others, a concept that could be called sustainable due diligence. As SWP argues, the due diligence norm is powerful given that, among other things, "[i]t expresses the cooperative and global character of a good international cyber and cybersecurity policy, without concealing its domestic foundations. Modern (cyber) foreign and security policies are always also domestic policies."[137] The same may be said for human rights, which is also being operationalized at multiple governance scales, from city ordinances to the U.S. Securities and Exchange Commission to the UN itself, a process that will likely continue to gain traction as awareness of the concept in both the public and private sectors is further raised.

However, for sustainable due diligence to reach its true and most comprehensive potential, more robust enforcement mechanisms must be put into place, as was stated in the UN GGE statement committing States to "stop [cyber] attacks that emanate from their territories and also commit to not deliberately damaging other countries' critical infrastructure or IT emergency teams."[138] The G2 cybersecurity code of conduct, 2016 G7 statement in support of cybersecurity norm building, and G20 list of cyber norms similarly provide fruitful ground on which to build out cybersecurity due diligence and further entrench it with human rights best practices, particularly as they relate to promoting the free flow of information, protecting privacy, and boosting economic development, all of which have been identified as being within the corpus of human rights law.[139] Furthermore, more work needs to be done on verification, transparency, and extraterritoriality in the sustainable due

135. INST. FOR HUMAN RIGHTS & BUS., *supra* note 1, at 3.

136. *Id.*

137. Bendiek, *supra* note 75, at 31.

138. *Id.*

139. *See* Communiqué, *supra* note 80; *G7 Leaders Approve Historic Cybersecurity Agreement*, BOSTON GLOBAL F (June 6, 2016), http://bostonglobalforum.org/2016/06/g7-leaders-produce-historic-cybersecurity-agreement/; Teri Robinson, *U.S., China Agree to Cybersecurity Code*

diligence context comprising cybersecurity, data privacy, and human rights considerations, lest we set out on a "collision course for different national legal systems, which would encourage the fragmentation of the global economic space and the Internet."[140] Deeper information sharing is also a vital component of an integrated due diligence norm, such as the pooling of cyber incident data into a repository that the public and private sectors can use to anonymously "share, store, aggregate, and analyze sensitive" cyber threat data as well as best practices.[141] Ultimately, countries and companies, policymakers and directors must come together to practice sustainable due diligence through polycentric governance if the broader goals of avoiding harm, as well as promoting human rights and cyber peace, are to be achieved.

of Conduct, SC MAG. (June 26, 2015), http://www.scmagazine.com/us-china-summit-talks-turn-to-cybersecurity/article/423175/; *see also* G.A. Res. 217 (III) A, pmbl., arts. 12, 23, Universal Declaration on Human Rights (Dec. 10, 1948), http://www.un.org/en/universal-declaration-human-rights/.

140. Bendiek, *supra* note 75, at 32.

141. *See* DEP'T HOMELAND SEC., Enhancing Resilience through Cyber Incident Data Sharing and Analysis: The Value Proposition for Cyber Incident Data Repository 2 (2015), https://www.dhs.gov/sites/default/files/publications/dhs-value-proposition-white-paper-2015_v2.pdf.